

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE

**Electricity metering – Payment systems –  
Part 41: Standard transfer specification (STS) – Application layer protocol for  
one-way token carrier systems**

**Comptage de l'électricité – Systèmes de paiement –  
Partie 41: Spécification de transfert normalisé (STS) – Protocole de couche  
application pour les systèmes de supports de jeton unidirectionnel**



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2014 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

### About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

### About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

#### IEC Catalogue - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

#### IEC publications search - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

#### IEC Glossary - [std.iec.ch/glossary](http://std.iec.ch/glossary)

More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: [csc@iec.ch](mailto:csc@iec.ch).

### A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

### A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

#### Catalogue IEC - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

#### Recherche de publications IEC - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 14 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

#### Glossaire IEC - [std.iec.ch/glossary](http://std.iec.ch/glossary)

Plus de 55 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

#### Service Clients - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: [csc@iec.ch](mailto:csc@iec.ch).



**INTERNATIONAL  
STANDARD**

**NORME  
INTERNATIONALE**

**Electricity metering – Payment systems –  
Part 41: Standard transfer specification (STS) – Application layer protocol for  
one-way token carrier systems**

**Comptage de l'électricité – Systèmes de paiement –  
Partie 41: Spécification de transfert normalisé (STS) – Protocole de couche  
application pour les systèmes de supports de jeton unidirectionnel**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

PRICE CODE  
CODE PRIX

ICS 17.220.20; 35.100.70; 91.140.50

ISBN 978-2-8322-1487-9

**Warning! Make sure that you obtained this publication from an authorized distributor.  
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

## CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	13
2 Normative references .....	13
3 Terms, definitions and abbreviations .....	14
3.1 Terms and definitions.....	14
3.2 Abbreviations.....	15
3.3 Notation and terminology .....	17
4 Numbering conventions .....	18
5 Reference model for the standard transfer specification .....	19
5.1 Generic payment meter functional reference diagram .....	19
5.2 STS protocol reference model.....	20
5.3 Dataflow from the POSApplicationProcess to the TokenCarrier.....	21
5.4 Dataflow from the TokenCarrier to the MeterApplicationProcess .....	22
5.5 MeterFunctionObjects / companion specifications .....	23
5.6 ISO transaction reference numbers.....	23
6 POSToTokenCarrierInterface application layer protocol.....	24
6.1 APDU: ApplicationProtocolDataUnit.....	24
6.1.1 Data elements in the APDU.....	24
6.1.2 MeterPAN: MeterPrimaryAccountNumber .....	25
6.1.3 TCT: TokenCarrierType .....	27
6.1.4 DKGA: DecoderKeyGenerationAlgorithm.....	27
6.1.5 EA: EncryptionAlgorithm.....	27
6.1.6 SGC: SupplyGroupCode.....	28
6.1.7 TI: TariffIndex.....	28
6.1.8 KRN: KeyRevisionNumber .....	29
6.1.9 KT: KeyType.....	29
6.1.10 KEN: KeyExpiryNumber .....	29
6.1.11 DOE: DateOfExpiry.....	29
6.2 Tokens.....	30
6.2.1 Token definition format .....	30
6.2.2 Class 0: TransferCredit.....	30
6.2.3 Class 1: InitiateMeterTest/Display .....	31
6.2.4 Class 2: SetMaximumPowerLimit.....	31
6.2.5 Class 2: ClearCredit .....	31
6.2.6 Class 2: SetTariffRate .....	31
6.2.7 Class 2: Set1stSectionDecoderKey.....	32
6.2.8 Class 2: Set2ndSectionDecoderKey.....	32
6.2.9 Class 2: ClearTamperCondition .....	32
6.2.10 Class 2: SetMaximumPhasePowerUnbalanceLimit.....	33
6.2.11 Class 2: SetWaterMeterFactor.....	33
6.2.12 Class 2: Reserved for STS use.....	33
6.2.13 Class 2: Reserved for Proprietary use .....	33
6.2.14 Class 3: Reserved for STS use.....	33

6.3	Token data elements .....	34
6.3.1	Data elements used in tokens .....	34
6.3.2	Class: TokenClass .....	35
6.3.3	SubClass: TokenSubClass .....	35
6.3.4	RND: RandomNumber .....	36
6.3.5	TID: TokenIdentifier .....	36
6.3.6	Amount: TransferAmount .....	38
6.3.7	CRC: CyclicRedundancyCode .....	39
6.3.8	Control: InitiateMeterTest/DisplayControlField .....	40
6.3.9	MPL: MaximumPowerLimit .....	41
6.3.10	MPPUL: MaximumPhasePowerUnbalanceLimit .....	41
6.3.11	Rate: TariffRate .....	41
6.3.12	WMFactor: WaterMeterFactor .....	41
6.3.13	Register: RegisterToClear .....	41
6.3.14	NKHO: NewKeyHighOrder .....	41
6.3.15	NKLO: NewKeyLowOrder .....	41
6.3.16	KENHO: KeyExpiryNumberHighOrder .....	41
6.3.17	KENLO: KeyExpiryNumberLowOrder .....	41
6.3.18	RO: RolloverKeyChange .....	42
6.4	TCDUGeneration functions .....	42
6.4.1	Definition of the TCDU .....	42
6.4.2	Transposition of the Class bits .....	42
6.4.3	TCDUGeneration function for Class 0,1 and 2 tokens .....	43
6.4.4	TCDUGeneration function for Set1stSectionDecoderKey token .....	44
6.4.5	TCDUGeneration function for Set2ndSectionDecoderKey token .....	46
6.5	Security functions .....	47
6.5.1	General requirements .....	47
6.5.2	Key attributes and key changes .....	47
6.5.3	DecoderKey generation .....	55
6.5.4	STA: EncryptionAlgorithm07 .....	60
6.5.5	DEA: EncryptionAlgorithm09 .....	64
7	TokenCarriertoMeterInterface application layer protocol .....	64
7.1	APDU: ApplicationProtocolDataUnit .....	64
7.1.1	Data elements in the APDU .....	64
7.1.2	Token .....	65
7.1.3	AuthenticationResult .....	65
7.1.4	ValidationResult .....	65
7.1.5	TokenResult .....	66
7.2	APDUExtraction functions .....	67
7.2.1	Extraction process .....	67
7.2.2	Extraction of the 2 Class bits .....	67
7.2.3	APDUExtraction function for Class 0 and Class 2 tokens .....	68
7.2.4	APDUExtraction function for Class 1 tokens .....	69
7.2.5	APDUExtraction function for Set1stSectionDecoderKey and Set2ndSectionDecoderKey tokens .....	69
7.3	Security functions .....	70
7.3.1	Key attributes and key changes .....	70
7.3.2	DKR: DecoderKeyRegister .....	70
7.3.3	STA: DecryptionAlgorithm07 .....	71

7.3.4	DEA: DecryptionAlgorithm09 .....	74
7.3.5	TokenAuthentication .....	74
7.3.6	TokenValidation.....	75
7.3.7	TokenCancellation .....	75
8	MeterApplicationProcess requirements .....	76
8.1	General requirements .....	76
8.2	Token acceptance/rejection .....	76
8.3	Display indicators and markings.....	77
8.4	TransferCredit tokens .....	78
8.5	InitiateMeterTest/Display tokens .....	78
8.6	SetMaximumPowerLimit tokens.....	78
8.7	ClearCredit tokens .....	79
8.8	SetTariffRate tokens .....	79
8.9	Set1stSectionDecoderKey tokens .....	79
8.10	Set2ndSectionDecoderKey tokens .....	79
8.11	ClearTamperCondition tokens.....	79
8.12	SetMaximumPhasePowerUnbalanceLimit tokens .....	80
8.13	SetWaterMeterFactor.....	80
8.14	Class 2: Reserved for STS use tokens .....	80
8.15	Class 2: Reserved for Proprietary use tokens .....	80
8.16	Class 3: Reserved for STS use tokens .....	80
9	KMS: KeyManagementSystem generic requirements .....	80
10	Maintenance of STS entities and related services.....	81
10.1	General.....	81
10.2	Operations .....	83
10.2.1	Product certification maintenance .....	83
10.2.2	DSN maintenance.....	83
10.2.3	RO maintenance.....	83
10.2.4	TI maintenance.....	84
10.2.5	TID maintenance .....	84
10.2.6	SpecialReservedTokenIdentifier maintenance .....	84
10.2.7	MfrCode maintenance.....	84
10.2.8	Substitution tables maintenance .....	84
10.2.9	Permutation tables maintenance.....	84
10.2.10	SGC maintenance .....	84
10.2.11	VendingKey maintenance .....	84
10.2.12	KRN maintenance.....	84
10.2.13	KT maintenance .....	84
10.2.14	KEN maintenance.....	85
10.2.15	KEK maintenance .....	85
10.2.16	CC maintenance .....	85
10.2.17	UC maintenance.....	85
10.2.18	KMCID maintenance.....	85
10.2.19	CMID maintenance .....	85
10.2.20	CMAC maintenance.....	85
10.3	Standardisation.....	86
10.3.1	IIN maintenance .....	86
10.3.2	TCT maintenance .....	86
10.3.3	DKGA maintenance .....	86

10.3.4	EA maintenance .....	86
10.3.5	TokenClass maintenance.....	86
10.3.6	TokenSubClass maintenance.....	87
10.3.7	InitiateMeterTest/DisplayControlField maintenance.....	87
10.3.8	RegisterToClear maintenance.....	87
10.3.9	STS base date maintenance .....	87
10.3.10	Rate maintenance.....	87
10.3.11	WMFactor maintenance .....	87
10.3.12	MFO maintenance .....	88
10.3.13	FOIN maintenance.....	88
10.3.14	Companion specification maintenance .....	88
Annex A (informative) Guidelines for a KeyManagementSystem (KMS).....		89
Annex B (informative) Entities and identifiers in an STS-compliant system.....		92
Annex C (informative) Code of practice for the implementation of STS-compliant systems .....		96
C.1	Maintenance and support services provided by the STS Association.....	96
C.2	Key management.....	96
C.2.1	Key management services .....	96
C.2.2	SupplyGroupCode and VendingKey distribution .....	96
C.2.3	CryptographicModule distribution.....	97
C.2.4	Key expiry .....	98
C.3	MeterPAN .....	98
C.3.1	General practice .....	98
C.3.2	IssuerIdentificationNumbers .....	98
C.3.3	ManufacturerCodes .....	98
C.3.4	DecoderSerialNumbers.....	99
C.4	SpecialReservedTokenIdentifier.....	99
C.5	Permutation and substitution tables for the STA.....	99
C.6	EA codes .....	99
C.7	TokenCarrierType codes.....	99
C.8	MeterFunctionObject instances / companion specifications .....	100
C.9	TariffIndex .....	100
C.10	STS-compliance certification.....	100
C.10.1	IEC certification services .....	100
C.10.2	Products .....	100
C.10.3	Certification authority.....	100
C.11	Procurement options for users of STS-compliant systems .....	100
C.12	Management of TID Rollover.....	104
C.12.1	Introduction .....	104
C.12.2	Overview .....	105
C.12.3	Impact analysis.....	107
C.12.4	Base dates .....	107
C.12.5	Implementation .....	107
Bibliography.....		110
Figure 1 – Functional block diagram of a generic single-part payment meter.....		19
Figure 2 – STS modelled as a 2-layer collapsed OSI protocol stack.....		20
Figure 3 – Dataflow from the POSApplicationProcess to the TokenCarrier .....		21

Figure 4 – Dataflow from the TokenCarrier to the MeterApplicationProcess .....	22
Figure 5 – Composition of ISO transaction reference number .....	23
Figure 6 – Transposition of the 2 Class bits .....	42
Figure 7 – TCDUGeneration function for Class 0, 1 and 2 tokens.....	43
Figure 8 – TCDUGeneration function for Set1stSectionDecoderKey token .....	44
Figure 9 – TCDUGeneration function for Set2ndSectionDecoderKey token .....	46
Figure 10 – DecoderKey changes – state diagram .....	52
Figure 11 – DecoderKeyGenerationAlgorithm01.....	57
Figure 12 – DecoderKeyGenerationAlgorithm02.....	58
Figure 13 – DecoderKeyGenerationAlgorithm03.....	59
Figure 14 – STA: EncryptionAlgorithm07.....	60
Figure 15 – STA encryption substitution process.....	61
Figure 16 – STA encryption permutation process .....	62
Figure 17 – STA encryption DecoderKey rotation process.....	62
Figure 18 – STA encryption worked example for TransferCredit token .....	63
Figure 19 – DEA: EncryptionAlgorithm09 .....	64
Figure 20 – APDUExtraction function.....	67
Figure 21 – Extraction of the 2 Class bits.....	68
Figure 22 – STA DecryptionAlgorithm07 .....	71
Figure 23 – STA decryption permutation process .....	71
Figure 24 – STA decryption substitution process.....	72
Figure 25 – STA decryption DecoderKey rotation process.....	73
Figure 26 – STA decryption worked example for TransferCredit token .....	73
Figure 27 – DEA DecryptionAlgorithm09 .....	74
Figure A.1 – KeyManagementSystem and interactive relationships between entities.....	89
Figure B.1 – Entities and identifiers deployed in an STS-compliant system .....	92
Figure C.1 – System overview .....	105
Table 1 – Data elements in the APDU .....	24
Table 2 – Data elements in the IDRecord.....	25
Table 3 – Data elements in the MeterPAN .....	25
Table 4 – Data elements in the IAIN / DRN .....	26
Table 5 – Token carrier types .....	27
Table 6 – DKGA codes .....	27
Table 7 – EA codes.....	28
Table 8 – SGC types and key types .....	28
Table 9 – DOE codes for the year .....	30
Table 10 – DOE codes for the month .....	30
Table 11 –Token definition format.....	30
Table 12 – Data elements used in tokens.....	34
Table 13 – Token classes .....	35
Table 14 – Token sub-classes .....	36
Table 15 – TID calculation examples .....	37

Table 16 – Units of measure for electricity .....	38
Table 17 – Units of measure for other applications .....	38
Table 18 – Bit allocations for the TransferAmount .....	39
Table 19 – Maximum error due to rounding .....	39
Table 20 – Examples of TransferAmount values for credit transfer .....	39
Table 21 – Example of a CRC calculation .....	40
Table 22 – Permissible control field values .....	40
Table 23 – Selection of register to clear .....	41
Table 24 – Classification of vending keys .....	48
Table 25 – Classification of decoder keys .....	49
Table 26 – Permitted relationships between decoder key types .....	53
Table 27 – Definition of the PANBlock .....	55
Table 28 – Data elements in the PANBlock .....	55
Table 29 – Definition of the CONTROLBlock .....	55
Table 30 – Data elements in the CONTROLBlock .....	56
Table 31 – Range of applicable decoder reference numbers .....	56
Table 32 – List of applicable supply group codes .....	57
Table 33 – Sample substitution tables .....	61
Table 34 – Sample permutation table .....	62
Table 35 – Data elements in the APDU .....	65
Table 36 – Possible values for the AuthenticationResult .....	65
Table 37 – Possible values for the ValidationResult .....	66
Table 38 – Possible values for the TokenResult .....	66
Table 39 – Values stored in the DKR .....	70
Table 40 – Sample permutation table .....	71
Table 41 – Sample substitution tables .....	72
Table 42 – Entities/services requiring maintenance service .....	82
Table A.1 – Entities that participate in KMS processes .....	89
Table A.2 – Processes surrounding the payment meter and DecoderKey .....	90
Table A.3 – Processes surrounding the CryptographicModule .....	90
Table A.4 – Processes surrounding the SGC and VendingKey .....	91
Table B.1 – Typical entities deployed in an STS-compliant system .....	93
Table B.2 – Identifiers associated with the entities in an STS-compliant system .....	94
Table C.1 – Data elements associated with a SGC .....	97
Table C.2 – Data elements associated with the CryptographicModule .....	98
Table C.3 – Items that should be noted in purchase orders and tenders .....	101

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

**ELECTRICITY METERING – PAYMENT SYSTEMS –****Part 41: Standard transfer specification (STS) –  
Application layer protocol for one-way token carrier systems**

## FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

International Standard IEC 62055-41 has been prepared by IEC technical committee 13: Electrical energy measurement and control.

This second edition cancels and replaces the first edition issued in 2007. It constitutes a technical revision. The main technical changes with regard to the previous edition are as follows:

- Class 2 token is extended to include credit transfer for gas and water with associated extensions in the display/test tokens.
- MfrCode is extended from 2 to 4 digits.
- Three token identifier base dates are defined to provide for more frequent key changes with TID roll-over procedures.
- A code of practice for the management of TID roll-over key changes in association with the revised set of base dates.
- Some clarifications and additional examples have been added.

The text of this standard is based on the following documents:

CDV	Report on voting
13/1530/CDV	13/1553/RVC

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

A list of all parts in the IEC 62055 series, published under the general title *Electricity metering – Payment systems*, can be found on the IEC website.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

This document is a preview generated by EVS

## INTRODUCTION

The IEC 62055 series covers payment systems, encompassing the customer information systems, point of sale systems, token carriers, payment meters and the respective interfaces that exist between these entities. At the time of preparation of this standard, IEC 62055 comprised the following parts, under the general title, *Electricity metering – Payment systems*:

Part 21: Framework for standardization

Part 31: Particular requirements – Static payment meters for active energy (classes 1 and 2)

Part 41: Standard transfer specification – Application layer protocol for one-way token carrier systems

Part 51: Standard transfer specification – Physical layer protocol for one-way numeric and magnetic card token carriers

Part 52: Standard transfer specification – Physical layer protocol for a two-way virtual token carrier for direct local connection

Part 4x series specify application layer protocols and Part 5x series specify physical layer protocols.

The standard transfer specification (STS) is a secure message protocol that allows information to be carried between point of sale (POS) equipment and payment meters and it caters for several message types such as credit, configuration control, display and test instructions. It further specifies devices and codes of practice that allow for the secure management (generation, storage, retrieval and transportation) of cryptographic keys used within the system.

The token carrier, which is not specified in this part of IEC 62055, is the physical device or medium used to transport the information from the POS equipment to the payment meter. Three types of token carriers are currently specified in IEC 62055-51 and IEC 62055-52; the magnetic card, the numeric token carrier and a virtual token carrier, which have been approved by the STS Association. New token carriers can be proposed as new work items through the National Committees or through the STS Association.

Although the main implementation of the STS is in the electricity supply industry, it inherently provides for the management of other utility services such as water and gas. It should be noted that certain functionalities may not apply across all utility services, for example, MaximumPowerLimit in the case of a water meter. Similarly, certain terminology may not be appropriate in non-electrical applications, for example, Load Switch in the case of a gas meter. Future revisions of the STS may allow for other token carrier technologies like smart cards and memory keys with two-way functionality and to cater for a real-time clock and complex tariffs in the payment meter.

Not all the requirements specified in this standard are compulsory for implementation in a particular system configuration and as a guideline, a selection of optional configuration parameters are listed in Clause C.11.

The STS Association is registered with the IEC as a Registration Authority for providing maintenance services in support of the STS (see Clause C.1 for more information).

Publication of IEC 62055-41 Ed 1 in May 2007 resulted in its rapid adoption as the preferred global standard for prepayment meters in many IEC member countries and a majority of IEC affiliate member countries. Prepayment electricity meters and their associated Payment Systems are now produced, operated and maintained by an ecosystem of utilities, meter manufacturers, meter operators, vending system providers, vending agents, banking institutions and adjacent industries. Multi-stakeholder interests are served by the STS Association comprising of more than 130 organisations located in over 24 countries. Interoperability and conformance to the Standard Transfer System (STS) are guaranteed by

Conformance test specifications developed and administered by the STS Association. A full list of the STS Association services can be found at <http://www.sts.org.za>.

Developed originally for prepayment electricity meters in Africa – via an IEC TC13 WG15 D-type liaison with the STS Association – this IEC standard now serves more users in Asia than Africa, with a total of approximately 35 million meters operated by 400 utilities in 30 countries. Management of the technology has been administered by the STS Association in fulfilment of its role as the IEC appointed Registration Authority.

Global success has brought about an urgent need to extend the range of the numerical elements contained in IEC 62055-41 tables. In particular, the range of manufacturer numbers need to be extended beyond the 99 numbers originally provided. Also, application of the standard has been extended to cater for multi-energy systems including gas and water meters. Accordingly, there is a need to ensure that the content of IEC 62055-41 is maintained to cater for this market growth and multi-energy extensions.

Several corrections and clarifications are also required to bring Ed 1 up to date with current practice. This was considered by TC13 WG15 at its meeting on the 20 September 2012 in London, where it was agreed that IEC 62055-41 should be revised.

Only the most urgently required revisions have been incorporated in Edition 2 due to timing constraints, but it is anticipated that Edition 3 will consider further revisions to incorporate the following functionalities:

- Currency transfer
- Enhanced security on par with contemporary industry practice
- Complex functions fully harmonized with DLMS/COSEM suite
- Decentralized key management system with distributed architecture
- Conformance certification test suite in conjunction with IEC CB scheme

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning special reserved token identifier given in 6.3.5.2.

IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the IEC that he/she is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with IEC. Information may be obtained from:

Address: Itron Measurement and Systems, P.O. Box 4059, TygerValley 7536, Republic of South Africa  
Tel: +27 21 928 1700  
Fax: +27 21 928 1701  
Website: <http://www.itron.com>

Address: Conlog (Pty) Ltd, P.O. Box 2332, Durban 4000, Republic of South Africa  
Tel: +27 31 2681141  
Fax: +27 31 2087790  
Website: <http://www.conlog.co.za>

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

ISO ([www.iso.org/patents](http://www.iso.org/patents)) and IEC (<http://patents.iec.ch>) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this International Standard may involve the use of a maintenance service concerning encryption key management and the stack of protocols on which the present International Standard IEC 62055-41 is based [see Clause C.1.] The IEC takes no position concerning the evidence, validity and scope of this maintenance service.

The provider of the maintenance service has assured the IEC that he is willing to provide services under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the provider of the maintenance service is registered with the IEC. Information may be obtained from:

Address: The STS Association, P.O. Box 868, Ferndale 2160, Republic of South Africa

Tel: +27 11 061 5000

Fax: +27 86 679 4500

Email: [sts@vdw.co.za](mailto:sts@vdw.co.za)

Website: <http://www.sts.org.za>

## ELECTRICITY METERING – PAYMENT SYSTEMS –

### Part 41: Standard transfer specification (STS) – Application layer protocol for one-way token carrier systems

#### 1 Scope

This part of IEC 62055 specifies the application layer protocol of the STS for transferring units of credit and other management information from a point of sale (POS) system to an STS-compliant payment meter in a one-way token carrier system. It is primarily intended for application with electricity payment meters without a tariff employing energy-based tokens, but may also have application with currency-based token systems and for services other than electricity.

It specifies:

- a POS to token carrier interface structured with an application layer protocol and a physical layer protocol using the OSI model as reference;
- tokens for the application layer protocol to transfer the various messages from the POS to the payment meter;
- security functions and processes in the application layer protocol such as the Standard Transfer Algorithm and the Data Encryption Algorithm, including the generation and distribution of the associated cryptographic keys;
- security functions and processes in the application layer protocol at the payment meter such as decryption algorithms, token authentication, validation and cancellation;
- specific requirements for the meter application process in response to tokens received;
- a scheme for dealing with payment meter functionality in the meter application process and associated companion specifications;
- generic requirements for an STS-compliant key management system;
- guidelines for a key management system;
- entities and identifiers used in an STS system;
- code of practice for the management of TID roll-over key changes in association with the revised set of base dates;
- code of practice and maintenance support services from the STS Association.

It is intended for use by manufacturers of payment meters that have to accept tokens that comply with the STS and also by manufacturers of POS systems that have to produce STS-compliant tokens and is to be read in conjunction with IEC 62055-5x series.

STS-compliant products are required to comply with selective parts of this International Standard only, which is the subject of the purchase contract (see also Clause C.11).

NOTE Although developed for payment systems for electricity, the standard also makes provision for tokens used in other utility services, such as water and gas.

#### 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050 (all parts), *International Electrotechnical Vocabulary* (available at <<http://www.electropedia.org>>)

IEC 62051:1999, *Electricity metering – Glossary of terms*

IEC 62055-21:2005, *Electricity metering – Payment systems – Part 21: Framework for standardization*

IEC 62055-31:2005, *Electricity metering – Payment systems – Part 31: Particular requirements – Static payment meters for active energy (classes 1 and 2)*

IEC 62055-51:2007, *Electricity metering – Payment systems – Part 51: Standard transfer specification (STS) – Physical layer protocol for one-way numeric and magnetic card token carriers*

IEC 62055-52:2008, *Electricity metering – Payment systems – Part 52: Standard transfer specification (STS) – Physical layer protocol for a two-way virtual token carrier for direct local connection*

ISO/IEC 7812-1:2006, *Identification cards – Identification of issuers – Part 1: Numbering system*

ISO/IEC 7812-2:2007, *Identification cards – Identification of issuers – Part 2: Application and registration procedures*

ANSI X3.92-1981, *American National Standard Data Encryption Algorithm, American National Standards Institute – Data Encryption Algorithm*

FIPS PUB 46-3:1999, *Federal Information Processing Standards Publication – Data Encryption Standard*

### **3 Terms, definitions and abbreviations**

#### **3.1 Terms and definitions**

For the purposes of this document, the terms and definitions given in IEC 60050, IEC 62051, IEC 62055-31 as well as the following apply.

NOTE Where there is a difference between the definitions in this standard and those contained in other referenced IEC standards, then those defined in this standard take precedence.

The term “meter” is used interchangeably with “payment meter”, “prepayment meter” and “decoder”, where the decoder is a sub-part of an electricity payment meter or a multi-part payment meter.

The term “POS” is used synonymously with “CIS”, “MIS” and “HHU” in the sense that tokens may also be generated by, and transferred between these entities and the payment meter.

The term “utility” is used to signify the supplier of the service in a general sense. In the liberalized markets the actual contracting party acting as the “supplier” of the service to the consumer may not be the traditional utility as such, but may be a third service provider party.

##### **3.1.1**

###### **companion specification**

specification managed by the STS Association, which defines a specific instance of a MeterFunctionObject (see 5.5 and Clause C.8)